encore networks™

Revision A, March 2010

© 2010 Encore Networks, Inc.
All rights reserved.

VSR-1200™ and RDU™ Installation and Quick Configuration Guide

2nd of 2 QuickStart™ Guides for the VSR-1200™

This guide presents procedures for a standard installation of the VPN Satellite Router™ 1200 (VSR-1200™) in the BANDIT family.

Note: The screens shown in this document are examples; the choices shown on your VSR-1200's menus depend on the features in the chassis and on the software version installed in the device. (For figures, tables, and configurations not addressed in this *Installation Guide*, see the Configuration Module or the BANDIT Products General Hardware Reference Module.)

See the following sections:

- *Before Installation*
- *Setting Up the Hardware*
- *Logging In*
- *Using the Main Menu*
- *Configuring the Software*
- *Saving (Writing) the Device's Configuration*
- *Restarting (Resetting) the Device*
- *Exiting a Session*

2.1 Before Installation

Gather all required information. Before you start these procedures, make sure you have all the information required to set up the VSR-1200 for use in your network—for example:

- The device's IP address
- The device's passwords
- The device's VPN configuration, if any
- Interface requirements for the device's ports
- Interface types for the ports—for example, DTE or DCE

- Interface protocols for the ports
- Network and routing functions that the device will perform
- Other pertinent network information

Use the *Site Planning Worksheets* as checklists for this information.

If you have questions or concerns after you have followed these procedures, contact Encore Networks, Inc., at *support@encorenetworks.com*, 703-787-4625 (fax), or 703-318-4350 (voice).

2.2 Setting Up the Hardware

1 Unpack the chassis and components from the shipping box. Make sure you have all the parts:

- the chassis (Figure 2-1)
- (if ordered) one or two RDU peripheral devices
- an RJ-45 Supervisory cable
- an adapter for the Supervisory cable (described in the Note in Step 8)
- a paper copy of this *Installation Guide*
- any additional accessories that you ordered

Note: Shipments within North America include power cables for AC outlets. For shipments outside North America, contact your distributor for cables that meet local requirements to connect the BANDIT's power supply to a power outlet.

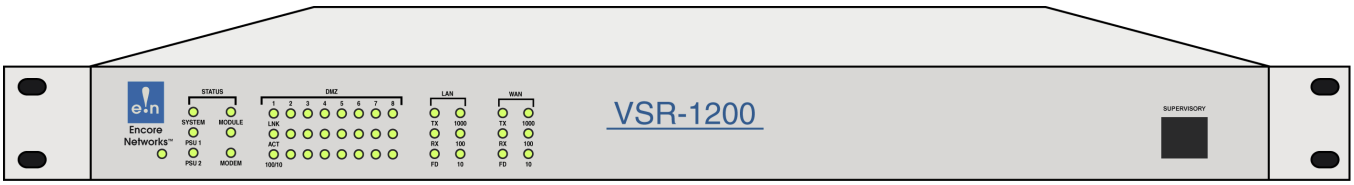

Figure 2-1. VSR-1200 Chassis, Front

2 Mount the VSR-1200 chassis in an equipment rack.

3 Connect an earth ground wire to the chassis, as follows: Attach a (minimum) 12 AWG wire to the earth ground screw (next to the safety ground symbol), on the extreme right rear or extreme left rear of the chassis (Figure 2-2). Use a ring terminal, such as an AMP (part number 36160), for this connection.

Warning: An earth ground must connect to the chassis so that the device remains grounded even when it is not receiving power.

Top Doc
Doc List
Module TOC

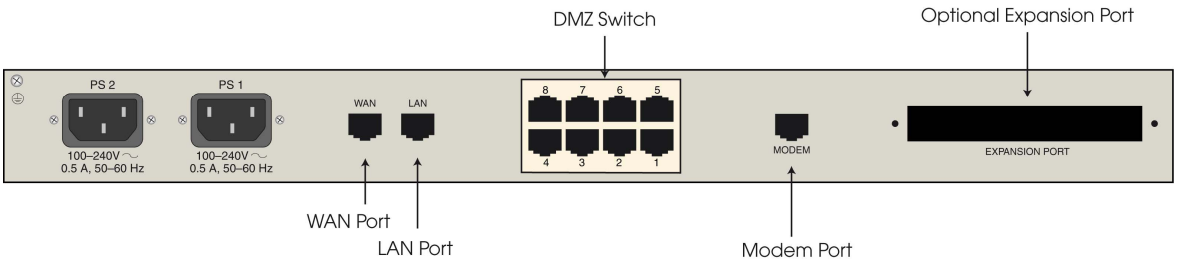

Figure 2-2. VSR-1200 Chassis, Rear

4 If this VSR-1200 uses one or two Remote Data Units™ (RDUs, Figure 2-3), connect each RDU's Ethernet port (Figure 2-4) to a separate Ethernet port on the VSR-1200's DMZ switch (Figure 2-2).

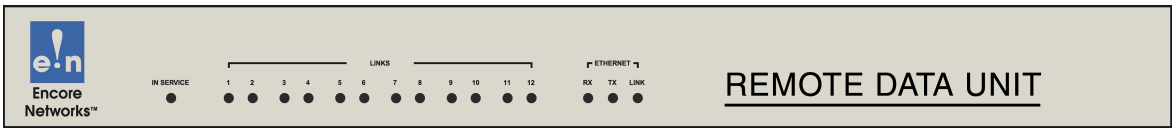

Figure 2-3. Remote Data Unit, Front

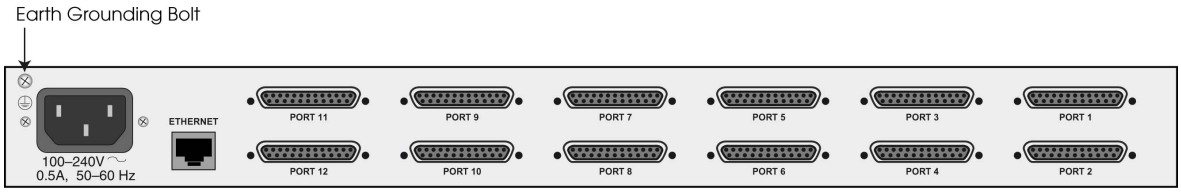

Figure 2-4. Remote Data Unit, Rear

5 Connect the VSR-1200's ports to their network devices.

6 If one or more RDUs are connected to the VSR-1200, connect each RDU's serial ports to their network devices.

7 Connect each power supply on the VSR-1200 chassis to an outlet supplying 100–240 VAC at 47–63 Hz.

8 Use the Supervisory cable and adapter to connect the device's Supervisory port to your PC's COM port.

Note: An eight-pin modular (RJ-45) to DB-9 adapter is the standard adapter to connect the Supervisory cable to a PC. This adapter is shipped with the unit. The following alternate adapters are also available. (Contact Encore Networks, Inc., if you need either of these adapters.)

- An RJ-45 to DB-25 adapter for connection to most asynchronous terminals
- An RJ-45 to DB-25 modem adapter to connect a modem, for out-of-band management or remote configuration

Top Doc
Doc List
Module TOC

2.3 Logging In

1 On the PC, open a terminal-emulation session, such as HyperTerminal. Use the settings in Table 2-1 to establish communication between the terminal console and the VSR.

Table 2-1. Supervisory Port Communication Settings

Parameter	Value
Bits per second	9600
Data bits	8
Parity	None
Stop bit	1
Flow control	Hardware

2 On the terminal console, press **Enter** to connect to the attached device.

❖ After successful log-in, the Main Menu appears.

2.4 Using the Main Menu

The Main Menu is displayed when you log onto the VSR. From the Main Menu, you can configure and operate the VSR.

```
Main Menu
----------
1) QuickStart Config Builder

2) Typical Configurations
3) Advanced Configurations
4) Tools

V) View Current Unit Status
L) Load Factory Defaults
P) Load Plug and Play Defaults
W) Write Configuration
R) Reset Unit
X) eXit Session
S) Statistics
Y) sYstem Administration

Enter Choice :
```

Note: Whenever you wish to return to a higher level in the VSR menus, press **Escape**.

! **Caution:** The Supervisory connection to the device will time out after five (5) minutes of console inactivity. If you have changed the device's configuration and wish to use the new configuration, save (write) the configuration before you leave the console. (See Section 2.6, *Saving (Writing) the Device's Configuration*.)

1 On the Main Menu, do one of the following:

a To set up a basic configuration of the VSR for your network, select **QuickStart Config Builders**.

❖ The Startup Config Options menu is displayed. (On the next menu—the Startup Configuration Scenarios menu—you can enter basic information; the VSR will use this information to build a standard configuration.) Go to Section 2.5.1, *Startup Configuration*.

```
Startup Config Options
----------------------
1) SATELLITE

Enter Choice :
```

b To configure specific features, select **Advanced Configurations**.

❖ The Advanced Configurations menu is displayed. You configure most parameters of the VSR from this menu. Go to Section 2.5, *Configuring the Software*.

```
Advanced Configurations
-----------------------
1) Physical Configurations
2) Data Configurations
3) Local Address
4) Routing
5) Global Paths

Enter Choice :
```

2.5 Configuring the Software

For a standard, basic configuration of the VSR for your network, see Section 2.5.1, *Startup Configuration*. For configuration of specific features, see the following sections.

- Section 2.5.2, *Device Addresses*
- Section 2.5.3, *Ports*
- Section 2.5.4, *Virtual Private Network Connections*
- Section 2.5.5, *IP Configuration*
- Section 2.5.6, *Simple Network Management Protocol*

2.5.1 Startup Configuration

The menu provides several templates for configurations that your network may use. You can select a template (also known as a startup scenario), change the scenario's IP addresses and related information to reflect the values in your network, and load the scenario into the VSR.

Note: If you want the device to keep the configured scenario, be sure to write (save) the configuration and reset the device.

Top Doc
Doc List
Module TOC

To configure a basic setup for this device in your network, do the following:

1 On the Main Menu, select **QuickStart Config Builders**.

2 On the Startup Config Options menu, select the set of configuration templates.

❖ The menu for Startup Configuration Scenarios appears.

```
Startup Configuration Scenarios
-------------------------------------
1) Ethernet WAN SLE Gateway(Initiator)
2) Ethernet WAN SLE Gateway(Initiator) With Dial Backup
3) Ethernet WAN SLE Gateway(Terminator)
4) Ethernet WAN SLE Gateway(Terminator) With Dial Backup

Enter Choice :
```

3 Select one of the listed set-ups.

❖ The menu for the selected set-up (scenario) is displayed. (The menu shown is for an **Ethernet WAN SLE Gateway, Initiator**.)

```
Startup Configuration Parameters
--------------------------------
1) System Name          :
2) LAN Interface IP    : 0.0.0.0        /0.0.0.0        No DHCP Server
3) LAN Private NAT IP  : 0.0.0.0         /0.0.0.0         masq:0.0.0.0
4) WAN Interface IP    : Dynamic
5) Primary DNS Server  : 0.0.0.0
6) VPN Gateway          :
7) VPN User ID          :
8) VPN Pre-Shared Key  :
9) Application Clients IP    : 0.0.0.0

L) Load Above Config
V) reView/Modify Loaded Config
R) Reset (Write and Reset)
Z) Clear All Fields

Enter Choice :
```

Note: At this point, all IP addresses, etc., have null values. Before you can load the configuration into the VSR, you must enter values that reflect your network's settings.

4 For each item (parameter) in the menu, do the following:

a Select the item (for example, **WAN Interface IP**).

```
Enter IP Address :
```

b Type a value for the item, and press **Enter**.

Top Doc
Doc List
Module TOC

c If the item requests additional information, enter that information.

❖ When the item has been configured, the scenario's menu is displayed again.

5 After you have performed Step 4 for each item (parameter) in the menu, do one of the following:

a Select **Load Above Config**.

❖ The following prompt asks for confirmation. Go to Step 6.

```
Caution: Existing configurations will be over written
Do you want to Continue?(Y/N)[N]:
```

b Select **Reset (Load, Write and Reset)**.

❖ The following prompt asks for confirmation. Go to Step 6.

```
Caution: Existing configurations will be over written
Do you want to Continue?(Y/N)[N]:
```

c Select **Clear All Fields**.

❖ The following prompt asks for confirmation.

```
This Clears All the above Fields, Continue?(Y/N)[N]:
```

- Do one of the following:
  - If you wish to reconfigure, enter **Y**.

❖ All fields in the menu are reset to null values. Return to Step 4.

- If you do not wish to reconfigure, press **Escape** to return to the Startup Configuration Scenarios menu.

❖ The configuration retains the settings you have entered, but they are not yet in use. Return to Step 4.

6 To load the new configuration, enter **y**.

❖ The configuration is loaded into the VSR.

Note: When you write (save) a configuration entered on the Quickstart menu, other required settings are updated automatically. For example, when you enter the device's IP address, a path is automatically set up in the IP routing table to direct this IP address to the device's LAN port.

❖ If you selected **Reset (Load, Write, and Reset)**, the configuration is also saved. This makes the configuration permanent (unless you change it again). Then the device resets.

7 When the configuration has finished loading, press **Escape** until you return to the Main Menu. (Go to Section 2.4, *Using the Main Menu*.)

8 To save the configured scenario (if it has not already been saved), do the following:

a **Write** the configuration. (See Section 2.6, *Saving (Writing) the Device's Configuration*.)

b **Reset** the device. (Section 2.7, *Restarting (Resetting) the Device*.)

2.5.2 Device Addresses

To configure the device's addresses, do the following:

1 On the Advanced Configurations menu, select **Local Addresses**.

```
BANDIT Plus
Configure Local Addresses
---------------------------
1) IP Address : 192.168.169.1
2) BANDIT Name : BANDIT Plus

Enter Choice :
```

2 On the Configure Local Addresses menu, select **IP Address**.

3 Enter the device's IP address and press **Enter**. (Get the device's IP address from your network administrator.)

4 Select **BANDIT Name**.

5 Enter a unique name to identify this device in your network, and press **Enter**.

2.5.3 Ports

To configure software for the device's ports, do the following:

1 On the Advanced Configurations menu, select **Data Configuration**.

❖ The Logical Port Protocol menu is displayed. (Table 2-2 lists the Line IDs for the ports.)

Table 2-2. Port Identifiers *(Sheet 1 of 2)*

Line ID	Physical (Hardware) Port	Default Software Configuration
C	COM/Supervisor port	Comm/Supervisor [a]
L	Ethernet LAN port	Ethernet
W	Ethernet WAN port	Ethernet

Top Doc
Doc List
Module TOC

Table 2-2. Port Identifiers *(Sheet 2 of 2)*

Line ID	Physical (Hardware) Port	Default Software Configuration
E	Expansion port	
B	RDU ports	(See Step 2.)
P	More ports [b]	(See Step 2.)

a. Do not modify the configuration for the Comm/Supervisor port.
b. These are virtual Logical Ports. A protocol configured on a Logical Port can be associated with a global path, which is turn is associated with a physical port. (See Section 2.5.3.1, *Protocols*. For information on global paths, see Section 4.3, *Defining Global Paths*, in *Port Configuration*.)

2 On the Logical Port Protocol menu, select the physical port whose software configuration you wish to modify.

❖ One of the following occurs:

- If you are configuring a physical port on the chassis, the Logical Port Attribute menu appears. Go to Step 4.
- If you are configuring a physical port on an RDU, the RDU Logical Port Menu is displayed. Continue to Step 3.

```
BANDIT Plus
Logical Port Protocol      Attached To                  Port Interfaces
-------------------------------------------------------------------------
1) UNDEFINED               RDU Port 1
2) UNDEFINED               RDU Port 2
3) UNDEFINED               RDU Port 3
4) UNDEFINED               RDU Port 4
5) UNDEFINED               RDU Port 5
6) UNDEFINED               RDU Port 6
7) UNDEFINED               RDU Port 7
8) UNDEFINED               RDU Port 8
9) UNDEFINED               RDU Port 9
A) UNDEFINED               RDU Port 10
B) UNDEFINED               RDU Port 11
C) UNDEFINED               RDU Port 12

Enter Port :
```

- If you are configuring a virtual Logical Port, the Virtual Logical Port menu is displayed. Continue to Step 3.

```
Logical Port Protocol       Mapped To                   Port Interfaces
-------------------------------------------------------------------------
 1) UNDEFINED
 2) UNDEFINED
 3) UNDEFINED
 4) UNDEFINED
 5) UNDEFINED
 6) UNDEFINED
 7) UNDEFINED
 8) UNDEFINED
 9) UNDEFINED
10) UNDEFINED
11) UNDEFINED
12) UNDEFINED
13) UNDEFINED
14) UNDEFINED
15) UNDEFINED
16) UNDEFINED
17) UNDEFINED
 P) More Ports...

Enter Port :
```

3 On the RDU Port menu or the Virtual Logical Port menu, select the port to configure.

❖ The Logical Port Attribute menu appears.

4 To modify the port's default settings, see the following:

- Section 2.5.3.1, *Protocols*
- Section 2.5.3.2, *DHCP Settings* (only for the WAN and LAN ports)
- Section 2.5.3.3, *Dial Backup Settings*

2.5.3.1 Protocols

To change the protocol that a port uses, or to modify attributes of a port's protocol, do the following on the Logical Port Attribute menu (see Section 2.5.3, *Ports*):

1 If you wish to change the protocol the port uses, do all of the following:

a Select **Undefine Current Logical Port**.

b Select **Protocol**.

c On the Logical Port Protocol Selection menu, select the protocol you want this port to use. Go to Step 2a.

2 To modify parameters in the port's protocol, select **Protocol**.

❖ The protocols available for the port are displayed.

a On the protocol configuration menu, select and change parameters to work in your network.

Top Doc
Doc List
Module TOC

b When you have finished configuring the protocol, press **Escape** to return to the Logical Port Attribute menu.

2.5.3.2 DHCP Settings

To review settings that the WAN or LAN port uses for DHCP, or to modify or disable DHCP on a port, do the following on the port's Logical Port Attribute menu (see Section 2.5.3, *Ports*).

Note: The WAN and LAN ports use different settings. Typically, a BANDIT device is a DHCP client on the WAN port and is a DHCP server on the LAN port. You may enable, modify, or disable use of DHCP on one port or on both ports.

1 Select **DHCP Type**.

❖ The DHCP Type menu appears.

```
DHCP Type
----------
1) Server
2) Client
3) None

Enter Choice :
```

2 Select the option you want this port to use.

❖ If you select **None**, the device does not use this port for DHCP. Press **Escape** until you return to the port's Logical Port Attribute menu. Go to Step 5.

❖ If you select **Client**, the device uses this port to request its IP address. (On the WAN port, the device requests its *public* IP address.) No further configuration is required for the DHCP client role. Press **Escape** until you return to the port's Logical Port Attribute menu. Go to Step 5.

❖ If you select **Server**, the device uses this port to assign IP addresses. (On the LAN port, the device assigns *private* IP addresses.) The Logical Port Attribute menu is redisplayed, with a menu item for configuring the DHCP server.

3 Select **DHCP Server Parameters**.

❖ The DHCP Server Parameters menu appears.

```
DHCP SERVER PARAMETERS
--------------------------

 1) Local DHCP Server IP Address (N.N.N.N):0.0.0.0
 2) DHCP Pool IP Address Low (N.N.N.N) :0.0.0.0
 3) DHCP Pool IP Address High (N.N.N.N) :0.0.0.0
 4) DHCP Network Mask (N.N.N.N) :255.255.255.0
 5) DHCP Lease Time (minutes) : 1440
 6) Domain Name for DHCP clients:
 7) Primary Router (N.N.N.N) :0.0.0.0
 8) NETBIOS Server (N.N.N.N) :0.0.0.0
Enter the number of the item to change:
```

4 Select and configure each parameter the device will use as the local (intranet) DHCP server. When you have finished configuring the DHCP server, press **Escape** until you return to the port's Logical Port Attribute menu.

5 When you have finished configuring the port, press **Escape** until you return to the Main Menu.

6 Save the configuration and reset the device. See Section 2.6, *Saving (Writing) the Device's Configuration*, and Section 2.7, *Restarting (Resetting) the Device*.

2.5.3.3 Dial Backup Settings

1 To configure a port for dial backup, select **Dialup Configuration** on the Logical Port Attribute menu (see Section 2.5.3, *Ports*).

Note: A port can be configured for dial backup only if its protocol supports dial backup. The port's Logical Port Attribute menu will not allow this option unless the protocol supports it. To select a protocol that supports dial backup, see Section 2.5.3.1, *Protocols*.

2 Configure the parameters for the dialup. When you have finished, press **Escape** to return to the Logical Port Attribute menu.

2.5.4 Virtual Private Network Connections

One of the principal features in the BANDIT family of products is the support of virtual private networks (VPNs). This section discusses the configuration of VPNs in the BANDIT products.

If any VPN connections will traverse satellite networks, the BANDIT uses Selective Layer Encryption™ (SLE, patent pending). See Section 2.5.4.3, *Selective Layer Encryption in VPNs*. The VSR products are dedicated to providing SLE VPN connections over satellite networks.

1 To configure VPN connections, do the following:

a On the Advanced Configurations menu, select **Routing.**

b On the Routing menu, select **IP Routing**.

c On the IP Routing Configuration menu, select **IP/VPN Routing**.

❖ The Virtual Private Network Configuration menu appears.

2 On the Virtual Private Network Configuration menu, do each of the following:

a To see the BANDIT device's list of VPN connections and associated security protocols, select **VPN Profiles**.

❖ The VPN Profile Table appears. Go to Section 2.5.4.1, *Configuring VPN Profiles*.

b To see the device's list of security policies for VPN connections, select **IP/VPN Policy Table**.

❖ The IP Policy menu appears. Go to Section 2.5.4.2, *Configuring the IP/VPN Policy Table*.

Note: You must also configure an IP routing table for use by the virtual private network. See Section 2.5.5.1, *IP Routing*.

Top Doc
Doc List
Module TOC

2.5.4.1 Configuring VPN Profiles

To configure VPN profiles, do the following:

1 On the Virtual Private Network Configuration menu, select **VPN Profiles**. (See Section 2.5.4, *Virtual Private Network Connections*.)

❖ The VPN Profile Table appears. Each VPN profile lists the following:

- The record number (line number)
- The VPN connection's profile name
- The tunneling mode the profile uses
- The IP address of the remote VPN gateway (the gateway at the other end of the VPN connection)
- The first negotiation scheme this local BANDIT device proposes for the connection

Note: For autokeyed connections, the table shows the authentication mode, authentication group, encryption protocol, and authentication protocol for Proposal 1 in Phase 1.

- Ping status
- The users allowed to use this VPN profile

2 Do one of the following:

a To change parts of a profile, type **m**. Go to Step 3.

b To add a profile, type **c**. Go to Step 4.

c To delete a profile, type **d**. Go to Step 5.

d To return to the Virtual Private Network Configuration menu, press **Escape**.

❖ The Virtual Private Network Configuration menu is redisplayed.

3 To modify an entry in the VPN Profile Table, do all of the following:

a Enter the line number of the profile to modify. (Line numbers are listed under the heading label **No.**)

❖ The fields for the selected VPN profile are displayed.

```
VPN PROFILE ENTRY
---------------------------
 1) Profile Name: AGGR_G2
 2) Tunneling Mode: AGGRESSIVE
 3) VPN Gateway: 0.0.0.0
 4) User ID:
 5) Pre-shared Key: *****
 6) Phase 1 Ping : Disabled     Idle Time: 120 seconds
 7) Phase 2 Ping : Disabled     Idle Time: 120 seconds
 8) Monitor Ping : Disabled     Idle Time: 120 seconds
 9) Phase 1 Proposal
10) Phase 2 Proposal

Enter the number of the item to change:
```

Top Doc
Doc List
Module TOC

Note: Although all VPN profile records have all fields, the screen displays only the fields used in the keying specified—autokeying (IKE) or manual. (The BANDIT VPN products do not use manual keying in normal operation. If you want a VPN device to use manual keying, contact your Encore Networks representative.)

b Type the line number of the field whose value you wish to change.

❖ If you select a phase proposal, a menu similar to the following is presented. Go to Section 2.5.4.1.1, *Configuring Phase Proposals for IKE Autokeying*.

```
Phase 1 Proposals
-------------------------
 1) Proposal 1: Preshared - DH GROUP G2 - DES  - HMAC-MD5
 2) Proposal 2: Preshared - DH GROUP G2 - DES  - HMAC-SHA1
 3) Proposal 3: Preshared - DH GROUP G2 - 3DES - HMAC-MD5
 4) Proposal 4: Preshared - DH GROUP G2 - 3DES - HMAC-SHA1
Enter your choice:
```

❖ If you select any other field, the field is presented, so that you may enter a new value.

c Type the new value for the field, and press **Enter**.

❖ The new value is accepted, and the selected profile is displayed with the new value.

d Do one of the following:

- If you wish to modify another field's value, return to Step 3b.
- When you have finished modifying this profile, press **Escape** to save the new values.

❖ The following prompt is displayed:

```
Do you want to keep your change? (Y/N):
```

e Do one of the following:

- To save the changes, press **y**.
- To discard the changes and keep the prior information, press **n**.

❖ Whether you answer **y** or **n**, the VPN Profile Table is redisplayed. Return to Step 2.

4 To add a profile to the VPN Profile Table, do all of the following:

a Type the line number of the existing profile you wish to copy as a model for the new profile.

b Type the name for the new profile, and press **Enter**.

Note: You may use profile names that are meaningful in your network—for example, **`Springfield Office`**, or **`Business Traveler 9`**.

❖ The software adds the new profile to the VPN Profile Table.

Top Doc
Doc List
Module TOC

c Return to Step 2.

5 To delete a profile from the VPN Profile Table, type the line number of the profile to delete. (Line numbers are listed under the heading label **No.**)

❖ The selected profile is deleted. The VPN Profile Table is redisplayed, minus the deleted profile. Return to Step 2.

2.5.4.1.1 Configuring Phase Proposals for IKE Autokeying

In VPN connections that use automatic keying (for example, Internet Key Exchange, or IKE), the BANDIT VPN device negotiates keys and proposals for data transmission. You can configure the proposals presented for each phase in the Internet Key Exchange.

To configure phase proposals for automatic keying, do the following:

1 On the VPN Profile Table, type **m** (to modify a line). Then type the line number and press **Enter**. (See Section 2.5.4.1, *Configuring VPN Profiles*.)

❖ The selected profile's fields are displayed.

2 Select the phase you wish to modify.

❖ The proposals already configured for the phase are listed.

3 Do one of the following:

a To return to the profile display, press **Escape**.

❖ The profile's list of fields is displayed. Go to Step 3d in Section 2.5.4.1, *Configuring VPN Profiles*.

b Select the proposal you wish to modify for this phase.

❖ The proposal's values are listed.

◆ Sample Phase 1 Proposal Menu:

```
Phase 1 Proposal 1
----------------------
 1) Authentication Mode : Preshared
 2) DH Group: DH GROUP G2
 3) Encryption: DES
 4) Authentication: HMAC-MD5
 5) Life: 100 sec
 6) Life Units: sec

Enter your choice:
```

- Sample Phase 2 Proposal Menu:

```
Phase 2 Proposal 1
--------------------
 1) PFS : DH GROUP G2
 2) Security Protocol: ESP
 3) Encryption: DES
 4) Authentication: HMAC-MD5
 5) Life: 100 sec
 6) Life Units: sec

Enter your choice:
```

4 Select the field whose value you wish to change, and press **Enter**.

❖ Possible values for the field are listed.

a Enter a new value for the field, and press **Enter**.

❖ The field's new value is accepted, and the proposal's values are listed again.

5 Do one of the following:

a To change another field's value, repeat Step 4.

b To return to the list of proposals configured for the selected phase, press **Escape**.

❖ The list of configured proposals is displayed again. Go to Step 3.

2.5.4.2 Configuring the IP/VPN Policy Table

You must configure the device's IP/VPN policy. This policy includes gateway connection information and the VPN profile that each connection uses.

If your connections will include VPNs across satellite networks, the BANDIT device will use selective layer encryption. Before configuring the IP/VPN Policy Table, read Section 2.5.4.3, *Selective Layer Encryption in VPNs*.

To configure the IP/VPN Policy Table, do the following:

1 On the Virtual Private Network Configuration menu, select **IP/VPN Policy Table**. (See Section 2.5.4, *Virtual Private Network Connections*.)

❖ The IP Policy menu appears.

2 On the IP Policy menu, do the following:

a Select **Status**, and **Enable** the IP/VPN policy table.

b Then select **Policy Table**.

❖ If the IP Policy Table does not yet have entries, it requests information for the first record. Go to Step 6b.

❖ If the IP Policy Table already has entries, the table is displayed.

```
       Source       Src    Destination     Dest   Protocol
#      Address      Port   Address         Port   /Flag    Path Name  I/O Action
--- -------------- ------ -------------- ------ -------- ---------- --- ------

  1        10.5.6.0    *        172.23.9.0    *          *     *        *
          10.5.6.255    *      172.23.9.255    *
    Tunnel To Remote 1 Action: Initiate VPN Profile: Remote

  2        *           *          *           *          *     *        *
           *           *          *           *
    Allow ALL Action: Allow

Add, Modify, Insert, Copy or Delete an Entry? - (A/M/I/C/D) : a
```

3 Do one of the following:

a To modify an entry, type **m**. Go to Step 4.

b To copy an entry, type **c**. Go to Step 5.

c To add an entry to the bottom of the list, type **a**. Go to Step 6.

d To add (insert) an entry at a specified point in the list, type **i**. Go to Step 7.

e To delete an entry, type **d**. Go to Step 8.

f To return to the Virtual Private Network Configuration menu, press the **Escape** key twice.

❖ The Virtual Private Network Configuration menu appears. Go to Section 2.5.4, *Virtual Private Network Connections*.

4 Do one of the following:

a To modify an entry, do all of the following:

- Type the line number of the entry you wish to modify.

❖ The entry's list of values appears.

- Select the field you wish to change.

❖ The possible values for the field are listed.

- Select the new value for the field.

❖ The new value is accepted, and the entry's list of values appears again.

b To return to the IP/VPN Policy Table, press the **Escape** key.

❖ A prompt asks whether you wish to save the changes you made.

c Answer **yes** (or **no**, if you decide not to keep the changes).

❖ The IP/VPN Policy Table appears. Return to Step 3.

5 Do one of the following:

a To copy an entry, type the line number of the entry you wish to copy.

❖ The new entry is added to the bottom of the IP/VPN Policy Table. Return to Step 3.

b If you do not wish to copy an entry, press the **Escape** key.

❖ The IP/VPN Policy Table appears. Return to Step 3.

6 To add an entry, do the following:

a If you do not wish to add another entry, press **Escape**.

❖ The IP/VPN Policy Table appears, with each new entry (if any) added to the bottom of the list. Return to Step 3.

b When screen prompts request information for this connection and its policy, type the information for each field, and press **Enter**.

Note: When asked for the profile name that this connection policy uses, you must enter a profile name that already exists in the VPN Profile Table. (To create new VPN profiles, see Section 2.5.4.1, *Configuring VPN Profiles*.)

❖ When all information has been entered, you are asked for a description.

c Type a name for the connection policy.

❖ The entry is accepted. A prompt appears for another new entry. Repeat Step 6.

7 To insert an entry, do the following:

❖ A prompt asks for the line number this entry will follow.

a Type the line number and press **Enter**.

❖ Subsequent prompts request information for this connection and its policy.

b Type the information for each field, and press **Enter**.

Note: When asked for the profile name that this connection policy uses, you must enter a profile name that already exists in the VPN Profile Table. (To create new VPN profiles, see Section 2.5.4.1, *Configuring VPN Profiles*.)

❖ When all information has been entered, you are asked for a description.

c Type a name for the connection policy.

❖ The entry is accepted, and the IP/VPN Policy Table appears, with the new entry inserted in the list at the specified location. Go to Step 3.

8 To delete an entry, type the entry's line number.

❖ The entry is deleted, and the IP/VPN Policy Table appears. Return to Step 3.

For more information, see the VPN Configuration Module.

2.5.4.3 Selective Layer Encryption in VPNs

Encore Networks has developed a proprietary technology, Selective Layer Encryption™ (SLE, patent pending), for VPNs that traverse a satellite network. SLE works with a satellite

groundstation's performance-enhancing proxy (PEP) and maintains VPN security over satellite networks. The use of SLE with PEP significantly increases IPsec performance over satellite networks. (For a discussion of SLE and satellite networks, see Section 1.4.3, *Selective Layer Encryption*, in *The BANDIT™ Products in Virtual Private Networks*.)

Figure 2-5 shows a sample satellite network combining PEP and SLE.

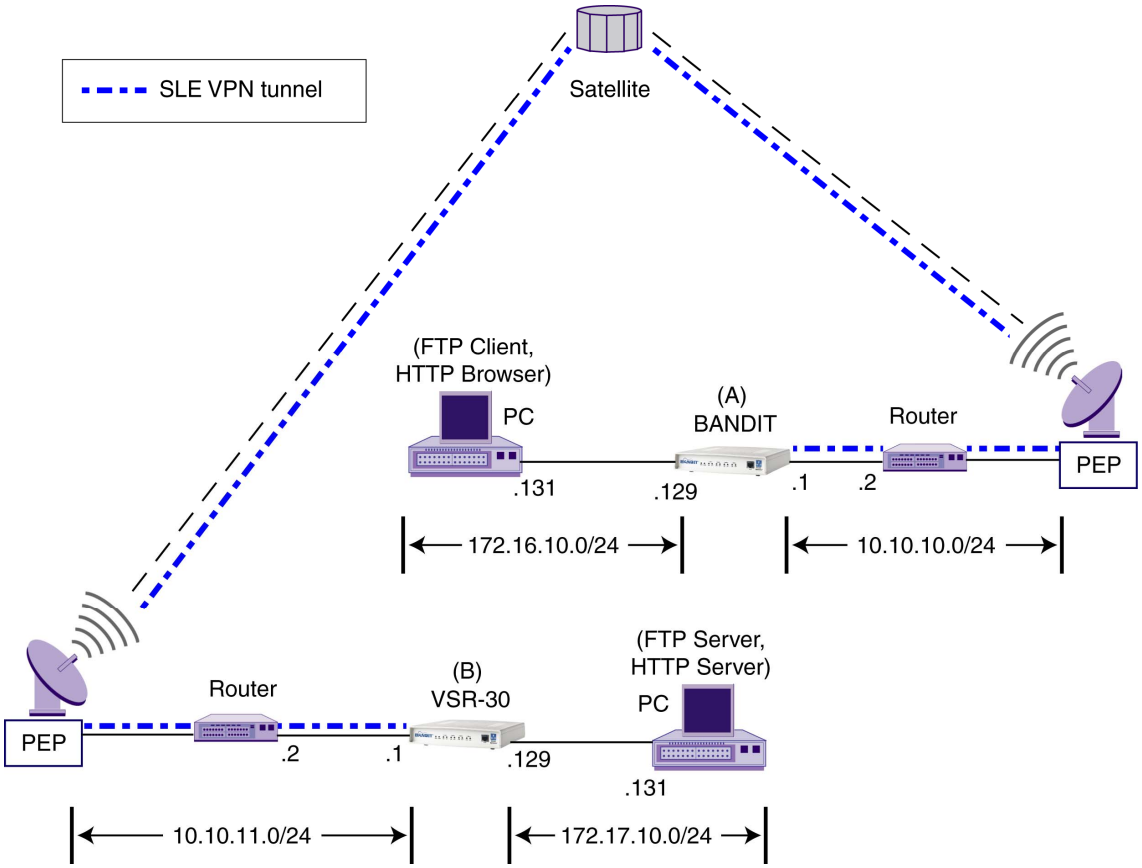

Figure 2-5. Sample Satellite Network Configuration Using Encore Networks' SLE VPN

2.5.4.3.1 SLE Configuration

The BANDIT products can use the following types of VPN software:

- The BANDIT's regular IPsec VPN software does not have SLE; all VPN tunnels in this software are IPsec without SLE. (This is the software the BANDIT IP uses.)
- The BANDIT's IPsec VPN software with SLE has everything; tunnels can use regular VPN or VPN with SLE. (This is the software the VSR products use. This software is also available in the BANDIT or the BANDIT Plus.)

The software for SLE differs slightly from the standard BANDIT software. However, the menus do not differ, and configuration remains the same for most parameters in the BANDIT.

Note: The VSRR-1200 is designed to support satellite networks as well as ground-based networks. Any BANDIT VPN device can support both VPN with SLE (for use over satellite networks) and VPN without SLE (for ground-based networks), depending on the software installed in the device. Most VPN devices can also support legacy applications.

The VSR-1200 is a high-end, high-performance router, and functions especially well as a hub for a large terrestrial (ground-based) or satellite network (or for a combined terrestrial–satellite network).

In the BANDIT's IPsec VPN software with SLE, all VPN tunnels use SLE, except in the following instance:

- In SLE software, in the IP Policy Table, if you select a record, the record's detail screen appears. Look at the name for the **Description**. If the description name begins with the letter "I" (upper case) or "i" (lower case), the configuration is IPsec VPN without SLE. (See Figure 2-10.) If the **Description** name begins with any other initial character, the configuration is IPsec VPN with SLE. (See Figure 2-7.)

  You configure both types of IPsec the same way, except for this parameter. All other items needed are configured automatically. (However, you need to supply the appropriate IP addresses.)

Note: In BANDIT software release 5.0 and above, the user does not configure FTP/HTTP ports 20, 21, and 80 for SLE. In addition, Network Address Translation is no longer required for SLE.

The user can modify the VPN configuration, if desired. We recommend consulting with your Encore Networks sales representative before modifying an automatically generated configuration.

Figure 2-6 shows part of the IP Policy Table for the BANDIT (A) in Figure 2-5. Note that record 3 is a catch-all policy for VPN with SLE; because it is a catch-all, it must follow all other records for VPN with SLE. Note that record 4 is a catch-all for VPN without SLE (and must follow all other records for VPN without SLE).

Figure 2-7 through Figure 2-10 show details of the records.

Top Doc
Doc List
Module TOC

```
       Source       Src    Destination     Dest   Protocol
#      Address      Port     Address       Port   /Flag    Path Name   I/O Action
--- -------------- ------ -------------- ------ -------- ----------- --- ------

  1   172.16.10.131    *        10.10.11.1    *          *     *        *
      172.16.10.131    *        10.10.11.1    *
    H-3 Action: Allow

  2   172.16.10.128    *        10.10.11.1    *          *     *        *
      172.16.10.255    *        10.10.11.1    *
    Tunnel To Remote 1 Action: Initiate VPN Profile: REMOTE

  3         *           *          *           *          *     *        *
            *           *          *           *
    H-1 Action: Allow

  4         *           *          *           *          *     *        *
            *           *          *           *
    I-Allow ALL Action: Allow
```

Figure 2-6. Sample Entries in IP Policy Table for BANDIT in Figure 2-5, Including SLE over Satellite Networks

```
1) Source Address Low : 172.16.10.131
   Source Address High : 172.16.10.131
   Source TCP/UDP Port Low :    *
   Source TCP/UDP Port High :    *
   Destination Address Low : 10.10.11.1
   Destination Address High : 10.10.11.1
   Destination TCP/UDP Port Low :   *
   Destination TCP/UDP Port High :   *
   Protocol/Flags :   *
   Path Name : *
   Incoming/Outgoing : *
   Filtering Action : Allow
   VPN Profile name : N/A
   Description : H-3
```

Figure 2-7. Detail of Record 1 in IP Policy Table, for SLE over Satellite Networks

```
2) Source Address Low : 172.16.10.128
   Source Address High : 172.16.10.255
   So Address Low : 10.10.11.1
   Destination Address High : 10.10.11.1
   Destination TCP/UDP Port Low :    *
   Destination TCP/UDP Port High :    *
   Protocol/Flags :   *
   Path Name : *
   Incoming/Outgoing : *
   Filtering Action : Initiate
   VPN Profile name : REMOTE
   Description : Tunnel To Remote 1
```

Figure 2-8. Detail of Record 2 in IP Policy Table, for SLE over Satellite Networks

```
3) Source Address Low : *
   Source Address High : *
   Source TCP/UDP Port Low :    *
   Source TCP/UDP Port High :    *
   Destination Address Low : *
   Destination Address High : *
   Destination TCP/UDP Port Low :     *
   Destination TCP/UDP Port High :     *
   Protocol/Flags :    *
   Path Name : *
   Incoming/Outgoing : *
   Filtering Action : Allow
   VPN Profile name : N/A
   Description : H-1
```

Figure 2-9. Detail of Record 3 in IP Policy Table, for SLE over Satellite Networks

```
4) Source Address Low : *
   Source Address High : *
   Source TCP/UDP Port Low :     *
   Source TCP/UDP Port High :     *
   Destination Address Low : *
   Destination Address High : *
   Destination TCP/UDP Port Low :     *
   Destination TCP/UDP Port High :     *
   Protocol/Flags : *
   Path Name : *
   Incoming/Outgoing : *
   Filtering Action : Allow
   VPN Profile name : N/A
   Description : I-Allow ALL
```

Figure 2-10. Detail of Record 4 in IP Policy Table, for IPsec VPN Traffic without SLE

Note: For VPN with SLE over satellites, there must be another BANDIT product using VPN with SLE on the other side of the network, handling SLE for the remote side of the connection.

Over ground-based networks, the BANDIT VPN products use non-SLE software and can interoperate with non-BANDIT IPsec VPN gateways. For details of IPsec interoperability, see *VPNC Scenario for IPsec Interoperability*.

2.5.5 IP Configuration

This section discusses additional IP components you must configure in order to use the VSR.

1. On the Advanced Configurations menu, select **Routing**.
2. On the Routing menu, select **IP Routing**.

   ❖ The IP Routing Configuration menu appears.

Top Doc
Doc List
Module TOC

3 See the following:

- Section 2.5.5.1, *IP Routing*
- Section 2.5.5.2, *IP Quality of Service*
- Section 2.5.5.3, *Network Address Translation*
- Section 2.5.5.4, *Firewall*

2.5.5.1 IP Routing

To use the VPN feature to its capacity, you must configure the device's IP routing. Do the following:

1 On the IP Routing Configuration menu, select the **IP Routing Method** you wish to use (**RIP** or **Static**).

2 On the IP Routing Configuration menu, do the following:

a If the IP routing method is **RIP**, select and configure **RIP Routing**. Follow the procedures for RIP routing in Section 2.1.2, *RIP Routing*, of *IP Routing in the BANDIT™ Products*.

```
 Entry  IP Address       Net Mask        Gpt Name     Next Router    Mode  MTU
---- -------------- --------------   ------------ -------------- ------  ----
 1   192.168.169.1   255.255.255.0    MODEM        0.0.0.0         Off    1500

Add, Modify, or Delete an Entry? (Enter A, M, or D):
```

b If the IP routing method is **Static**, select and configure **Static Routing**. Follow the procedure for static routing in Section 2.1.3, *Static Routing*, of *IP Routing in the BANDIT™ Products*.

```
Entry  IP Address      Net Mask        Next Router     Path Name  Hops
   1   1.2.3.4         255.0.0.0       Unnumbered      a          1

Add, Modify, or Delete an Entry? (Enter A, M, or D):
```

For more information, see *IP Routing in the BANDIT™ Products*.

2.5.5.2 IP Quality of Service

To use the VPN feature to its capacity, you must configure the device's IP Quality of Service. Do the following:

1 On the IP Routing Configuration menu, select **IP Quality of Service**.

2 On the IP Priority menu, select **Prioritization**.

3 On the IP Quality of Service menu, do the following:

a Select **Status**, and **Enable** IP quality of service.

b Select **Quality of Service Table**, and configure entries in the table.

```
      Source       Src      Destination    Dest
#     Address      Port     Address        Port   Protocol Path Name  Priority
--- -------------- ------ -------------- ------ -------- ---------- ----------

  1        *           *          *           *          *     *      Immediate
           *           *          *           *

           *           *          *           *

Add, Modify, Insert or Delete an Entry? - (A/M/I/D) :
```

c Set a **Default Priority** for IP packets that do not match any entry in the table.

For more information, see *IP Quality of Service* in the Routing Module.

2.5.5.3 Network Address Translation

You can use the BANDIT products for network address translation (NAT).

If your connections will include VPNs across satellite networks, the BANDIT device will use selective layer encryption. Before configuring the NAT Table, read Section 2.5.4.3, *Selective Layer Encryption in VPNs*.

To use network address translation, do the following:

1 On the IP Routing Configuration menu, select **Network Address Translation**.

2 On the Network Address Translation menu, do the following:

a Select a NAT configuration scheme.

b Enable and configure the NAT configuration scheme according to your network plan—e.g., for masquerading, or for a NAT table.

For more information, see *Network Address Translation* in the Address Translation Module.

2.5.5.4 Firewall

The default settings for the VSR do not use the firewall feature. If you wish to configure the firewall, do the following.

1 On the Main Menu, select **Typical Configurations**.

2 On the Typical Configurations menu, select **Configure Firewall**.

3 On the Configure Firewall menu, configure the policy table, NAT profiles, and IP interfaces for your network's dynamic firewall.

For more information, see the *The BANDIT™ Device as Firewall* in the Routing Module.

2.5.6 Simple Network Management Protocol

If you wish to use Simple Network Management Protocol (SNMP) with the VSR, do the following to configure the device's built-in SNMP agent:

1 On the Main Menu, select **System Administration**.

Top Doc
Doc List
Module TOC

2 When the system asks for your password, enter the default password and press **Enter**.

Note: If your product order requested a different, specific password, contact your system administrator for the password.

3 On the System Administration menu, select **SNMP Configuration**.

4 On the SNMP Configuration menu, do the following:

a Configure the **SNMP Get Community String**.

b Configure the **SNMP Set Community String**.

c Configure the **SNMP Trap Default Address**.

d Configure IP addresses for the **SNMP Trap Table**.

5 Now you can configure an SNMP manager on your control terminal. (Encore Networks does not furnish SNMP manager software.)

2.6 Saving (Writing) the Device's Configuration

Note: If you do not save the configuration before you reset or exit the VSR (or before the connection times out), the configuration will be lost.

After the unit has been configured, save (write) the configuration. Do the following:

1 On the Main Menu, select **Write Configuration**.

2 Select **Yes**.

❖ The device will notify you when it has saved the configuration.

Note: If the device's software detects an error in the configuration, it will not save it. Review the configuration. After you have revised the configuration to your satisfaction, save it.

3 Press **Enter**.

2.7 Restarting (Resetting) the Device

To use the saved configuration, you must reset the VSR. Do the following:

Note: If you want to use your new configuration, you must save (write) the configuration before resetting the unit. Otherwise, the new configuration will be lost.

1 On the Main Menu, select **Reset Unit**.

2 Select **Yes.**

Note: If you have not yet saved the new configuration, the system asks whether to save it. Answer **yes** or **no**.

❖ The device resets.

3 Regardless of screen instructions, do not type anything until you see the banner: ***BANDIT, ENCORE NETWORKS INC***. Then press **Enter**.

❖ The Main Menu is displayed.

2.8 Exiting a Session

After the software has been configured, save (write) the configuration. Then exit the session before disconnecting the PC, so that communication is not disrupted.

! **Caution:** Before you exit, make sure you save (write) the configuration. Otherwise, the changes you configured will be lost. See Section 2.6, *Saving (Writing) the Device's Configuration*.

To exit the session, do the following:

1 On the Main Menu, select **Exit Session**.

❖ The following prompt is displayed.

```
Are You Sure? :
```

2 Select **Yes**.

Note: If the configuration has not been saved, the device asks you whether it should save the new configuration. Answer **Yes** (or **No**, if you prefer not to save the configuration).

❖ The system notifies you that it is ending the session.

```
Ending Session...
```

Note: To reconnect to the device and start a new session, press **Enter**.

❖ The terminal's connection to the BANDIT starts up, and the BANDIT's Main Menu is displayed.